

# State of Connecticut



## Collaboration & Directory Services Domain

### Technical Architecture

January 4, 2001

Version 1.00

## History of Changes

Date	Modification
12/7/2000	Added descriptions for remaining component technologies
12/5/2000	Added Standard 7: XML Added Standard 8: DirXML Added DirXML to Product Status Table as a Pilot Strategic Product Added Appendix A: Directory Services Policy
11/28/2000	Added descriptions of component technologies for Basic Collaboration Services and Extended Collaboration Services Added section for Ongoing Architecture Development to identify known gaps in the domain architecture that will be in the team's work plan Changed Banyan StreetTalk to Obsolete Status in Product Status Table

## Table of Contents

<b>History of Changes .....</b>	<b>i</b>
<b>Table of Contents.....</b>	<b>ii</b>
<b>Mission.....</b>	<b>1</b>
<b>Introduction/Background.....</b>	<b>1</b>
<i>Background</i>	2
<b>Components .....</b>	<b>3</b>
1. <i>Basic Collaboration Services</i>	3
2. <i>Extended Collaboration Services</i>	3
3. <i>Process Management</i>	4
4. <i>Directory Services</i>	5
<b>Principles .....</b>	<b>8</b>
<b>Principle 1.</b> Basic Services for all employees	8
<b>Principle 2.</b> Classification of Content	8
<b>Principle 3.</b> Universal Access to Network Services	8
<b>Principle 4.</b> Architecture Governance	9
<b>Principle 5.</b> External Use of Collaborative Systems	9
<b>Principle 6.</b> Metrics Gathering and Analysis	9
<b>Principle 7.</b> Reduce Integration Complexity	9
<b>Principle 8.</b> Data and Process Integration and Sharing	10
<b>Principle 9.</b> Business Process Re-design	10
<b>Principle 10.</b> Consistent Configurations	10
<b>Principle 11.</b> Old Configuration Re-deployment	10
<b>Principle 12.</b> Component Re-Use	11
<b>Principle 13.</b> Partitions and Boundaries	11
<b>Principle 14.</b> Interfaces	11
<b>Principle 15.</b> Re-engineered Common Processes	12
<b>Principle 16.</b> Consistent Engineering Practices	12
<b>Principle 17.</b> Mainstream Technologies and Industry Standards	12
<b>Principle 18.</b> Business Continuity and Disaster Recovery	12
<b>Principle 19.</b> Virtual LAN	13

## Collaboration And Directory Services Domain Technical Architecture

<b>Principle 20.</b>	Scalability	13
<b>Principle 21.</b>	Interaction with Other Domains	13
<b>Principle 22.</b>	Relation to E-Government Domain	13
<b>Principle 23.</b>	End User Resource Limitations	14
<b>Principle 24.</b>	Reuse and Buy Before Build	14
<b>Principle 25.</b>	Use of Standard API's	14
<b>Principle 26.</b>	Review Cycle	14
<b>Principle 27.</b>	Minimize Searching for Information	15
<b>Principle 28.</b>	Appropriate Search and Retrieval Tools	15
<b>Principle 29.</b>	Minimize the number of Push Tools	15
<b>Principle 30.</b>	Document Exchange	15
<b>Principle 31.</b>	Collaboration Systems are Enterprise Solutions	16
<b>Principle 32.</b>	Common Directory Service	16
<b>Principle 33.</b>	Minimize Number of Languages	16
<b>Principle 34.</b>	Avoid Proprietary Languages	16
<b>Product and Technical Standards.....</b>		<b>17</b>
Standard 1:	Exchange 2000 Server with Outlook 2000 Mail Client	17
<i>Best Practice 1a:</i> .....		17
<i>Best Practice 1b:</i> .....		17
Standard 2:	FileNET Integrated Document Management Suite	18
Standard 3:	Novell Directory Services	18
Standard 4:	Simple Mail Transport Protocol (SMTP)	19
Standard 5:	Multi-purpose Internet Mail Extensions (MIME)	19
Standard 6:	Lightweight Directory Access Protocol (LDAP)	20
Standard 7:	Extensible Markup Language (XML)	20
Standard 8:	Novell DirXML	21
<b><i>Ongoing architecture Development</i></b>		<b>22</b>
Imaging		22
Computer Output to Laser Disk		22
Content Management		22
Workflow Integration		22
Electronic Mail Response Management		22
Directory Services		23
<b><i>Emerging Standards</i></b>		<b>24</b>

# Collaboration And Directory Services Domain Technical Architecture

Emerging 1: Internet Calendaring and Scheduling Core Object Specification (iCalendar)	24
Emerging 2: iCalendar Transport-Independent Interoperability Protocol (iTIP)	24
Emerging 3: iCalendar Message-Based Interoperability Protocol (iMIP)	25
<b>Collaboration &amp; Directory Services Product Status .....</b>	<b>26</b>
<b>Appendix A: Implementation and Deployment of Directory Services .....</b>	<b>29</b>

## **Mission**

The Collaboration and Directory Services Architecture exists to guide decisions about the appropriate use, implementation and management of these technologies so that the State's Conceptual Architecture Principles are realized. Conformance with those overarching principles will assure alignment of the technologies within this domain with the business requirements of the State and the creation of an adaptable collaboration environment that can readily change to meet the changing demands of the State's agencies and service programs.

## **Introduction/Background**

In the public sector, collaboration technologies enable organizations to create, share, and leverage accumulated information and knowledge across the entire spectrum of government entities and their associated service programs. Collaboration technologies provide the means for people-to-people communication and collaborative work, internally among State agencies as well as between State agencies and external entities (e.g. federal and municipal government organizations, 3<sup>rd</sup> party service providers, regulated entities, and Connecticut residents). Collaboration technologies are supported and complemented by enterprise-class directory services which provide infrastructure repositories for identity management, access control, resource identification and location, and management of relationships between named resources in the State's network. Together these technologies assist people in reducing the time and effort required to distribute ideas, notifications, proposals, and other documents throughout workgroups, across entire organizations or externally to service partners, clients, oversight groups or other interested parties.

Collaboration technologies provide the means to improve organizational effectiveness and workgroup performance through a variety of products that span the spectrum of human interaction styles from structured to improvisational. There are two major thrusts for the State's deployment of collaborative systems that are derived from the State of Connecticut Conceptual Architecture Principles:

Internally focused collaboration and communication, with a holistic state government perspective intended to eliminate barriers to information sharing created by the fragmented implementation of closed collaborative systems.

The extension of collaborative technologies to facilitate extra-enterprise sharing of information and processes (i.e. inter-organizational collaboration and communication with entities external to the State).

Traditional approaches to collaborative workgroup solutions typically have an intra-organizational focus that is oriented to paperwork reduction, improving the efficiency of processes and enhancing the quality of decisions. In the vision articulated by the Conceptual Architecture, State agency boundaries become irrelevant. The workgroup can be any virtual organization needed to accomplish the State's mission. Extra-enterprise communications encompass both structured and ad hoc means to share information and knowledge across organizational boundaries using the full spectrum of collaborative technologies. Both approaches recognize the role that technology-facilitated communication will play in the realization of the goals of electronic government. It also acknowledges the complexities of managing services delivered via public-private partnerships, which require a set of automated

## Collaboration And Directory Services Domain Technical Architecture

tools to facilitate collaborative planning and rapid problem resolution. These same technologies can also play a significant role in the delivery of distance learning services via the Internet.

As the State explores the potential benefits of widely deployed collaborative technologies, it must always be mindful of its legal and ethical obligations to protect the public interest and the privacy of its citizens. We must always balance the ease of creating shared environments with feature-rich collaboration tools against our responsibility as information stewards to ensure that all security requirements are met for the classes of information that will reside or move through those environments.

### Background

The critical issues to consider with respect to collaborative technology selection are the continuing shifts in government service delivery modalities, organizational relationships and technology management that are being driven by an increased need to respond quickly to high impact shifts in government policy at the federal and state level. These changes are generating tremendous demand for externalization of processes and information sharing across and beyond the State as an enterprise. Satisfying this demand requires a fundamental change in the way the State uses technology to realize strategic policy imperatives. It also requires a corresponding shift in the State's underlying value system that is embodied in the basic premise that information is valued as an enterprise asset, which must be shared to enhance and accelerate decision making.

Broad deployment of basic collaboration services (defined below) will form the foundation for collaborative applications that span government boundaries. These fundamental services will provide the foundation for a natural progression to real-time services such as network-based meetings, cross-repository searches, and multi-organizational content/knowledge management. Web user interfaces, portals, and coalescing standards (e.g. LDAP, HTML/XML) will be critical to integrating collaboration services with directory services and thereby permitting the externalization of processes and extra-enterprise information sharing in a controlled secure manner. As these technologies mature it is important for the State of Connecticut to be in a position to support the agencies, their service partners and their clients when they require more sophisticated electronic collaboration tools.

The principles in this document are intended to facilitate the evaluation, selection, design, construction, implementation and management of the domain technologies. The principles, standards and product selections for this domain affect and are affected by other domains. The principles with respect to these intersection points are included in this document.

## Components

The following descriptions of the technology components of this Domain are grouped by four major categories to provide a simple framework for understanding a complex and multi-faceted set of technologies. The State's Conceptual Architecture directs us to define a standardized set of basic information services to all employees, so we begin there with the identification of a set of basic services for the Collaboration Domain.

### 1. Basic Collaboration Services

Basic collaboration services support ad hoc people-to-people communication and coordination of activities in an electronic format. These basic services should be universally available to all State employees because they provide the tools to move information quickly among people regardless of their work location or work shift, to coordinate the activities of those people, and to support their need to work collaboratively. In the 21<sup>st</sup> century these are as basic to communication as the telephone was in the 20<sup>th</sup> century. These services include:

- Electronic Mail – transmits computer-based messages via local, regional or global networks.
- Calendar Sharing / Scheduling Common Resources – provides for electronic appointment books and To Do Lists with reminder alerts. Calendars for people, facilities and resources can be shared among groups of people to facilitate the coordination of group activities.
- Network-based Fax – provides a shared facsimile service accessed via the local network from a user's personal computer. It allows faxes to be sent from computer to fax machine, from fax machine to computer or from computer to computer without requiring a printed copy as an intermediate step.
- Shared folders/document sharing – provides common disk space with access controls to support simple document sharing without document management features such as version control, or rendering into other formats.
- Threaded discussions – creates links between electronic documents and responses to those documents as a record of an electronic dialogue occurring among people working in a collaborative process.
- Ad hoc work routing – allows users to create routing lists for documents that need to be sent to other users for review or editing.

### 2. Extended Collaboration Services

Extended collaboration services support ad hoc and structured communication among groups of people, and the sharing of their collective information resources. These services include:

- Integrated Document Management / Content Management – provides indexed, searchable repositories for all document types (e.g. word processing, spreadsheets, presentations, web pages) and is integrated with the personal computer software used to create those documents.
- Knowledge Management – an advanced application of collaborative technologies that provides a cultural and technological framework to capture and share knowledge about State programs, products and services. This collective knowledge is currently in people's minds (as personal knowledge and experience), on isolated paper documents and in segregated electronic storage.



## Collaboration And Directory Services Domain Technical Architecture

- Indexing, Search and Retrieval – are the keys to sharing and reusing information. Electronic files that are not classified appropriately and indexed are very difficult to find and use, especially in shared repositories with thousands of documents. Robust search and retrieval tools are necessary to manage multiple document repositories with complex access control requirements.
- Archive Management – provides the means to move electronic files off-line while preserving their access controls and retention schedule information. It also allows archived files to move back to an active storage location if necessary.
- Imaging – the creation, capture, storage and management of digital renderings of documents and photographs in standard image formats.
- Real Time Whiteboard – the electronic equivalent of a whiteboard, but on a computer screen that allows one or more users to draw on the screen while other users on the network watch.
- Network Meeting – supports online, moderated meetings during which participants can use a variety of conferencing tools to share desktop applications, record meeting notes, and distribute files, video and audio to participants. The technology also supports the use of real-time video.

### 3. Process Management

Process management technologies support the automation of well defined, rules-driven processes. These technologies include:

- Electronic Forms Processing – the use of workflow technologies for the automatic routing of electronic forms (e-forms) among a group of people responsible for processing them; the initiation of fully automated processing of information contained on e-forms; the validation or insertion of data on e-forms via database look-up; combinations of these three functions; plus audit trail creation, exception notifications and archive functions. Processes are in all cases well-defined and rules-driven, but can range from a simple series of sequential steps to multi-organizational, compound processes with conditional branching based on e-form content.
- Process-centric Workflow – the automated management of the flow of material, information, and knowledge through a well-defined process. The core of workflow is the automation of information-based tasks and activities, but workflow processes must also be able to keep track of non-electronic objects through their association with electronic identification (for example a barcode). Knowledge is captured in the rules that are embedded in the automated processes during its creation. These rules include schedules, priorities, routing paths, authorizations, security and the roles of all the people and computer systems in the process. The development environment for workflow includes analysis and design tools that facilitate change through rapid deployment of workflow applications and reuse of process elements.
- Electronic Mail Response Management - EMRM applications use artificial intelligence and business rules to read and sort inbound electronic inquiries, respond to simple questions, and escalate complex problems to the appropriate human agent. Human interaction plays a major role in electronic mail response management. People are necessary to solve complex problems and to respond to requests for help

from those frustrated by unexpected results when using self-service applications. The State must build systems that can capture and respond to electronic citizen inquiries quickly, efficiently and comprehensively. These systems should be able to deliver personalized responses and must scale easily to match rapid volume growth. This requires investments in service knowledgebases to support both the automated self-help interfaces and human intervention. These systems must also address security requirements driven by citizen expectations for privacy and protection of personal information. EMRM is a technology that is will be subsumed into customer interaction management suites (customer relationship management, call center management, direct mail, real-time Web interaction tools) over the next few years. See also the discussion of Consumer Relationship Management in the Web E-Government Domain Technical Architecture.

### 4. Directory Services

A directory service is a physically distributed, logically centralized repository of infrequently changing data that is used to manage a computing environment. Directory services provide the means to manage relationships between named resources in the State network by performing a variety of access governance roles. Robust security-driven directory services are essential to the externalization of processes and the extension of collaboration services to 3<sup>rd</sup> party service partners, regulated entities, citizens and other entities external to State government. Critical functions performed by directory services include:

- Authentication services including digital signature and non-repudiation – are used to verify the identity of a user or a computer system process. Digital signature systems allow people and organizations to electronically certify such features as their identity, their ability to pay, or the authenticity of an electronic document.  
Non-repudiation is achieved through cryptographic methods that provide proof of the integrity and origin of data that can be verified by any third party at any time or that with high assurance can be asserted to be genuine and that cannot subsequently be refuted.  
As a database of network-based resources, users; and the access rules that apply to them – directories define and enforce the relationships between named resources in the network, providing the foundation for centralized management of security.
- Single Sign On – through the use of well-known, widely accepted, standards-based cryptography, protocols and APIs provide a user with access to all authorized network resources, applications and information stores without having to locate and log in to each one individually.
- Directory enabled Network Management (DEN) - enhancing the usability and manageability of networks via integration with the directory service. In these networks, the network resources (devices, operating systems) use the directory to publish information about themselves, discover other resources, and obtain information about those other resources. The directory service becomes the hub around which distributed systems turn, enhancing the interoperability among network components and distributed applications and thereby providing predictable and repeatable service levels, strengthening security and improving network management.
- Access Profile Management – access profiles define access control lists for users and network based resources.

## Collaboration And Directory Services Domain Technical Architecture

- Quality of Service management – the directory can be used as a policy data store for determining prioritized levels of network services required and authorized for applications and users. Policy-based management leverages the power of directory services, providing solutions that deliver significant ease of use and allow administrators to standardize and automate configuration management. The Distributed Management Task Force (DMTF) and the Internet Engineering Task Force (IETF) are defining standards in this area. In the directory a policy is a virtual object associated with a group of configuration parameters. The policy object is then associated with a group of devices or services that receive those configuration parameters when the policy is enforced. Through the directory, administrators can manage a single set of configuration parameters—QoS configuration, for example—for a group of devices or services.
- On-demand, searchable listing of available resources – essentially a comprehensive electronic blue pages that would backend query systems on the Internet and intra-governmental network.
- Meta Directory – directory of directories, directory of data resources. Using the directory service as the repository for the complete glossary for all components, databases, fields, objects, owners, access, platforms and users within the enterprise. The repository offers a way to understand what information is available, where it is stored, its currency and other important facts about the data. See the Data Management and Data Warehouse Domain Technical Architecture for further discussion of metadata repositories.
- Certificate repository for Public Key Infrastructure – PKI uses a form of cryptography involving two related keys. The public key is openly available in a repository to anyone who wants to communicate with the user in a secure manner. The user's public key is distributed using an electronic document called a Public Key Certificate that also contains the user's name and an expiration date. See the Security Domain Technical Architecture for additional information on Public Key/ Private Key technology.
- Web portal personalization for classes of users and individual users - As portals try to personalize the experience for users, more and more information about the users can be stored in profiles. This information is not just static information like name and email address, but also the user's preferences, likes and dislikes, and also their usage patterns. In addition to dynamic information, user management also involves managing information about the organization the user belongs to or the role they are playing at the point of interaction (e.g. parent, client advocate, licensed professional, or town tax collector). Portals could also store access rights information for the user or the roles associated with them. There are a number of issues regarding privacy and confidentiality that must be addressed by government organizations before any significant use of portal personalization can be used.
- Directory management tools – robust, comprehensive management tools and the advanced training necessary to use them are essential to the successful deployment of integrated directory services.

## Collaboration And Directory Services Domain Technical Architecture

Because of the extensive interaction required of these technology components to create a collaborative environment, the principles that govern this domain are provided together in the next section.

## Principles

The following principles are provided to guide the State of Connecticut in the evaluation, selection, design, construction, implementation and management of the products and services within the Collaboration and Directory Services Domain.

### **Principle 1.** Basic Services for all employees

A standardized set of basic collaboration services will be provided to all employees as required to meet business needs.

#### ***Rationale***

- Increases productivity.
- Reduces costs of maintenance.
- Provides the basis for multi-agency or statewide business initiatives.
- Provides for universal employee access to information.
- Leverages the investments made in technology.

### **Principle 2.** Classification of Content

When designing collaborative systems (e.g. document management, workflow), the content that will move through the system must be classified according to applicable statutes, policies and regulations pertaining to availability, retention and security.

#### ***Rationale***

- Supports Conceptual Architecture Principle: *Information is valued as an enterprise asset, which must be shared to enhance and accelerate decision-making.*
- Information in collaborative systems is another type of State information that must be managed according to the same principles of stewardship as structured data.
- The State must minimize the exposure and liability of mismanaging information stored in collaborative systems.
- To make information easily shared, it must be classified.

### **Principle 3.** Universal Access to Network Services

Enterprise collaboration requires universal access to a robust set of integrated network infrastructure services.

#### ***Rationale***

- Content exchange, directory services, electronic mail communications and authentication services are key infrastructure components necessary for communication and collaboration.
- The infrastructure and communications backbone is critical for the widespread use of communication tools, conferencing tools, etc.
- These components must be in place in order to support the use of collaboration technologies.

### **Principle 4.**      Architecture Governance

The architecture governance process must assure that the State does not use collaborative tools for information management problems that are more appropriately solved by other technologies. For example, data warehouses must be used in place of collaborative tools where appropriate to eliminate unnecessary and uncontrolled replication of data.

#### ***Rationale***

- Technology choices must be made with full consideration of the information sharing and security requirements.
- There is a risk that collaborative technologies will be chosen as preferred solutions because they are readily available and familiar to staff in the agencies.
- The State must minimize the exposure and liability of mismanaging information stored in collaborative systems.

### **Principle 5.**      External Use of Collaborative Systems

When designing collaborative systems, consideration must be given to the possible use of that system by people outside the State enterprise (e.g. general public, 3rd party service providers).

#### ***Rationale***

- Supports direct access to information by constituents from multiple locations using multiple methods and media.
- Supports the delivery of training through mediated information and instruction where the teachers and students are not co-located; many agencies have training/education responsibilities that are central to their mission.
- The State is expected to move increasing amounts of constantly changing information out to a variety of audiences.
- Supports collaboration with clients and external service providers.
- Constituents may be sending confidential information via a collaborative system.
- The State must minimize the exposure and liability of mismanaging information stored in collaborative systems.

### **Principle 6.**      Metrics Gathering and Analysis

When designing workflow systems, metrics gathering and analysis capabilities should be built in.

#### ***Rationale***

- Enables an increase in the types and quantity of internal business metrics collected, monitored and analyzed for use by management.

### **Principle 7.**      Reduce Integration Complexity

The Collaboration and Directory Services Architecture must reduce integration complexity to the greatest extent possible.

## Collaboration And Directory Services Domain Technical Architecture

### ***Rationale***

- Increases the ability of the State to adapt to change.
- Reduces product implementation and support costs.

### **Principle 8. Data and Process Integration and Sharing**

Collaborative systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across the enterprise and with our external service partners.

### ***Rationale***

- Increases efficiency while better serving our customers (e.g. the public, agencies, etc.).
- Redundant systems cause higher support costs.
- Ensures more accurate information.
- Integration leads to better decision making and accountability.

### **Principle 9. Business Process Re-design**

New collaborative systems will be implemented after business processes have been analyzed, simplified or otherwise redesigned as appropriate.

### ***Rationale***

- Work processes will be more streamlined, efficient and cost effective.
- Work processes, activities, and associated business rules will be well understood and documented.
- Reduces the total cost of ownership.

### **Principle 10. Consistent Configurations**

Create a small number of consistent configurations for collaborative systems and directory services to be used across the State of Connecticut.

### ***Rationale***

- The cost of IT personnel is increasing and the cost of hardware is decreasing rapidly.
- This is the most efficient approach to enterprise-wide infrastructure configuration and maintenance.
- By constantly 'tweaking' the performance of individual systems, a multitude of unique configurations is created, thus increasing support and maintenance costs.
- Standardized decisions in product selection simplify training, reduce learning curves and maximize transferability of skills.

### **Principle 11. Old Configuration Re-deployment**

Old configurations should not be re-deployed (even to those with no technology) without a full consideration of the Total Cost (including support) of doing so.

### ***Rationale***

- Supports Conceptual Architecture Principle: *Adopt a total cost of ownership model for applications and technologies which balances the costs of development, support,*

## Collaboration And Directory Services Domain Technical Architecture

*training, disaster recovery and retirement against the costs of flexibility, scalability, ease of use, and reduction of integration complexity.*

### **Principle 12.** Component Re-Use

Groupware applications, collaborative systems and directory services will employ reusable components across the enterprise, using an n-tier model.

#### ***Rationale***

- Enables simplification of the environment and better integration with other technology domains.
- Hastens the delivery of systems to the agencies.
- Facilitates the creation of a consistent computer environment for agency staff.
- Takes advantage of modular off-the-shelf components.
- Reuse will lower costs and maintenance efforts.
- Allows for leveraging skills across the enterprise.
- For Workflow systems there is an equivalent “re-use” potential for the definition of a business event that is common to other business processes.

### **Principle 13.** Partitions and Boundaries

The logical design of application systems and databases should be highly partitioned. These partitions must have logical boundaries established, and the logical boundaries *must not be violated*.

#### ***Rationale***

- Collaborative systems must be designed so that they do not violate this principle even though there is a trend among collaborative technologies to blur the boundaries between them (e.g. contents of web stores, e-mail repositories and file sharing systems).
- Content storage decisions must balance control between the local end-user and the enterprise support unit because content storage choices can impact the potential for information sharing, disaster recovery, etc.

### **Principle 14.** Interfaces

The interfaces between separate application systems must be *message-based*; this applies to both internal and external systems.

#### ***Rationale***

- The use of messaging is important for enforcing the architecture principle of logical partitioning and boundaries.
- Messaging technology simplifies integration efforts.
- Workflow is inherently message based, however systems should still be designed to conform to this principle because of the likelihood of integration with existing applications systems.
- This principle also applies to this domain because of the potential for future interoperability between State collaborative systems and external collaborative systems (see Emerging Standards).



## Collaboration And Directory Services Domain Technical Architecture

- As a general practice, consistency in design philosophy across all systems will simplify the challenge of establishing a disciplined development environment.

### **Principle 15.** Re-engineered Common Processes

Re-engineered common processes should be used by all agencies in their Workflow systems.

#### ***Rationale***

- Supports the Conceptual Architecture Principle: We must deploy application *systems that are driven by business events*.
- There is an equivalent “re-use” potential for the definition of a business event that is common to other business processes.

### **Principle 16.** Consistent Engineering Practices

The State shall adopt and employ consistent software engineering practices and methods for the development of collaborative systems.

#### ***Rationale***

- Supports the Conceptual Architecture Principle: *The State shall adopt and employ consistent software engineering practices and methods based on accepted industry standards*.
- We need to strike a balance between being too rigid in the engineering of collaborative systems (stifling creativity) and the lack of discipline typically found in informal end-user development practices.

### **Principle 17.** Mainstream Technologies and Industry Standards

Collaborative systems will use industry-proven, mainstream technologies that adhere to industry standards and open architecture principles.

#### ***Rationale***

- Implementation of the Conceptual Architecture Principles: IT solutions will use industry-proven, mainstream technologies and Priority will be given to products adhering to industry standards and open architecture.
- These technologies are in a state of flux.
- Choosing proprietary systems may come at a higher cost to transfer to an open standard at a later date.
- Proprietary systems introduce integration complexity into the IT environment.

### **Principle 18.** Business Continuity and Disaster Recovery

All collaborative systems and directory services will have an associated business continuity plan and their design specifications will include provisions for disaster recovery that is appropriate to the criticality of the business functions they support.

#### ***Rationale***

- Implementation of the Conceptual Architecture Principle: An assessment of business recovery requirements is mandatory when acquiring, developing, enhancing or outsourcing systems.

## Collaboration And Directory Services Domain Technical Architecture

- Based on that assessment, appropriate disaster recovery and business continuity planning, design and testing will take place.

### **Principle 19.** Virtual LAN

Directory Services will be designed to support the use of the Statewide network as the gateway to secure anywhere, anytime access to information and services.

#### ***Rationale***

- Implementation of the Conceptual Architecture Principle: *We must implement a statewide backbone network that provides a virtual, enterprise-wide local area network.*
- Networks are the essential enabling technology for client/server, Internet, and collaborative computing.
- Knowledge workers' increasing need for access to information across the enterprise must be seamless in order to reduce decision-making cycle times.

### **Principle 20.** Scalability

Collaborative technologies and directory services must be scalable in size and capacity. Collaborative systems and directories should be designed to be extensible and portable across the platforms identified in the Platform Domain.

#### ***Rationale***

- Implementation of the Conceptual Architecture Principle: The underlying technology infrastructure and applications must be scalable in size, capacity, and functionality to meet changing business and technical requirements.
- The Total Cost of Ownership is minimized.
- Encourages reuse.
- Leverages the continuing decline in hardware costs.

### **Principle 21.** Interaction with Other Domains

Select tools and solutions that interact with, support or utilize the architectures of the other technology domains.

#### ***Rationale***

- This domain is an "integration domain".
- Rather than create specific data integration and middleware solutions that are separate from the rest of the architecture, we will leverage those that have been defined in these other technology domains.
- Collaborative systems and directories should function independently of the systems management concerns of the hardware upon which they reside, however their underlying software should support basic systems management activities such as logging for diagnostics and user tracking.
- This principle will lead us to select solutions that can be supported by these other domains.

### **Principle 22.** Relation to E-Government Domain

The principles for decision making within this domain must be blended with the principles for managing the E-Government domain.

## Collaboration And Directory Services Domain Technical Architecture

### ***Rationale***

- As an “integration domain”, this domain must interact with principles across other domain intersection points.
- As a domain that includes infrastructure services that will be used by the e-government environment it is imperative that the principles for these two domains remain in synch.

### **Principle 23. End User Resource Limitations**

Design solutions that consider the end user’s available bandwidth and client resources.

### ***Rationale***

- External or mobile users of these technologies may not be able to access content or applications at the same speed or in the same format as full clients on the network.
- One must be cognizant of these differentiating factors and design systems accordingly.

### **Principle 24. Reuse and Buy Before Build**

We will consider re-use of existing applications, systems and infrastructure before investing in new solutions. We will build only those applications or systems that will provide clear business advantages and demonstrable cost savings.

### ***Rationale***

- The availability of specific solutions in the collaborative technology space, such as customer relationship management packages will require that the State consider a “build versus buy” decision.
- Using tested solutions reduces risk.
- Reduces the Total Cost of Ownership.

### **Principle 25. Use of Standard API’s**

Collaboration software shall use standard Application Programming Interfaces (APIs).

### ***Rationale***

- In order to avoid the use of proprietary coding practices, it is important that the selected solutions use standards API’s.

### **Principle 26. Review Cycle**

The review cycle for these technologies is 6 months

### ***Rationale***

- These technologies are rapidly changing and maturing.
- The principles for this domain must be reviewed/revised every six months in order to keep up with this ever-changing technology space.
- In-depth research and aggressive technology assessment of changes in collaboration technologies is necessary because of the inherent vulnerabilities of these technologies which are designed to be open and easy to deploy.

### **Principle 27.** Minimize Searching for Information

Minimize the number of searches required for locating information throughout the State.

#### ***Rationale***

- Searching for information is usually frustrating if it has not been categorized and indexed to facilitate finding it.
- The more indices that are developed for known search criteria, the greater the possibility that the user community will find this service useful.
- Each search engine has its own unique approaches for providing this functionality.
- Product decisions and system design decisions must be based upon this principle.

### **Principle 28.** Appropriate Search and Retrieval Tools

Select search and retrieval tools appropriate to the collaboration environment.

#### ***Rationale***

- Search and retrieval tools are not yet technologically mature or robust enough to link all technologies and their repositories together.
- We should strive to minimize the number of search and retrieval tools needed to search the repositories within the collaboration space.
- The selected tools should be a natural extension of the collaboration environment and the desktop environment.

### **Principle 29.** Minimize the number of Push Tools

Seek to minimize the number of “push” tools for subscriptions.

#### ***Rationale***

- Although “pull” tools for querying information are specific to the type of collaboration required (i.e. searching through the e-mail system, querying a metadata system, searching discussion groups), the use of “push” tools is based upon published information and can interact with published information from disparate sources.
- With a number of tools now available, the selection and use of a limited number of tools should minimize the complexity of interaction with this information.

### **Principle 30.** Document Exchange

When sharing documents externally, use standardized formats to reduce content exchange conflicts.

#### ***Rationale***

- Content exchange is a critical Collaboration Technologies infrastructure component, enabling the exchange of electronic information and data between individual users and groups.
- It includes the interchange of editable and non-editable documents between applications and individuals.
- Establishing content exchange standards provides flexibility and independence when exchanging documents.

## Collaboration And Directory Services Domain Technical Architecture

- These standards enable a variety of tools to be used to view documents stored in standard formats.

### **Principle 31.** Collaboration Systems are Enterprise Solutions

Manage and select each collaboration system as if it is an enterprise solution.

#### ***Rationale***

- Collaboration systems typically start as a local self-contained collaborative applications, then expand in scope and become difficult to support from both an operational and application development perspective.
- The creation of collaboration systems based upon broader, enterprise considerations is more likely to produce adaptive systems.
- This is also supportive of the Conceptual Architecture Principle *Reduce Integration Complexity*.

### **Principle 32.** Common Directory Service

Leverage a common directory for internal communication and collaboration.

#### ***Rationale***

- An enterprise-wide directory service should be accessible by everyone within the organization.

### **Principle 33.** Minimize Number of Languages

The number of programming languages for any system will be minimized to reduce maintenance complexity.

#### ***Rationale***

- When developing collaborative systems, no one programming language is likely to provide all required functionality.
- Given the nature of the State's n-tier approach to application development, it is important to consider the increased level of maintenance complexity when multiple languages are used.
- Minimizing the number of languages used in collaboration systems will mitigate the associated risks and costs.

### **Principle 34.** Avoid Proprietary Languages

Whenever possible, use non-proprietary programming languages for collaborative systems.

#### ***Rationale***

- As stated, these technologies are in flux.
- In order to provide an adaptive range in the architecture, avoiding the use of proprietary languages will provide greater flexibility in shifting to other products, as these technologies become more mature and stable.

## Product and Technical Standards

The following product and technical standards have been established for the State of Connecticut. The Conceptual Architecture Principles and Requirements for Technical Architecture (RTA) that are supported by the standard are included in the explanation of the standard. The text for the RTAs is included at the end of the explanation for easy reference. Where best practices have been defined for the implementation of products, they are also included.

### **Standard 1: Exchange 2000 Server with Outlook 2000 Mail Client**

Microsoft Exchange 2000 is the State's strategic product for basic collaboration services such as e-mail, group calendars and scheduling, shared folders/document sharing, task management, threaded discussions, instant messaging, and ad hoc work routing (*RTA-10*). The use of a single product for these services supports a number of the conceptual architecture principles including:

- Reduce Integration Complexity
- Total Cost of Ownership
- Minimize Platform Configurations
- Basic Information Services
- Mainstream Technologies
- Industry Standards
- and Scalability.

The State is undertaking its first implementations of Exchange 2000 with pilots at the Department of Mental Retardation and the Department of Social Services. The implementation experience acquired during these two projects will be the basis for the development of detailed design principles and a set of best practices for future projects. The desktop client for e-mail will be Outlook 2000. The DMR pilot will determine the appropriate e-mail configuration for a thin client in the Citrix environment. Mobile employees will need a mobile thin client for remote access to the Exchange server (*RTA- 11*). Telecommuting employees will need a Web client for remote access from home. The Outlook Web Access client will be tested as a light weight choice for remote access. Both of these remote access scenarios will require careful consideration of the security issues involved in externalizing the Exchange environment. All other groupware products will be transitioned to Exchange 2000 over time, depending on agency readiness and funding to make the transition. Groupware applications for e-forms, process-centric workflow or document-centric workflow will transition over time to the State standard products for those types of systems (see Standard 3).

#### **Best Practice 1a:**

E-mail messages will be managed in server-based storage that has a regular back-up.

#### **Best Practice 1b:**

E-mail systems will be configured to permit easy classification of messages for archival purposes based on the State's Document Retention Guidelines as interpreted by each agency for their particular content.

RTA-10 EWTA will provide support for productive teamwork including file sharing, email, application sharing, white boarding, audio and video teleconferencing, and work routing.

## Collaboration And Directory Services Domain Technical Architecture

RTA-11 EWTA shall provide secure access to all computing and information resources for mobile workers.

### **Standard 2: FileNET Integrated Document Management Suite**

The FileNET Integrated Document Management Suite is the State's strategic product set for the following information management functions that meet the requirements of *RTA-13*:

- document management systems;
- document-centric workflow applications for document life cycle management;
- process-centric workflow applications for process management, including electronic forms processing;
- image management systems; and
- their supporting indexing, search and retrieval, and archive management services.
- This product set supports a number of the conceptual architecture principles including
  - Information is an Enterprise Asset
  - Reduce Integration Complexity
  - Total Cost of Ownership
  - Minimize Platform Configurations
  - Shared Components Using an N-Tier Model
  - Event-Driven Systems
  - Mainstream Technologies
  - Industry Standards
  - and Scalability.

The State is undertaking its first implementations of the FileNET Integrated Document Management Suite with projects at the Department of Labor and the Department of Environmental Protection. An electronic forms application was recently tested at the Office of Policy and Management. The State has a small installed base of older FileNET document management systems. The implementation experience acquired during construction of these older systems plus the new knowledge garnered during the new projects will be the basis for the development of detailed design principles and a set of best practices for future projects.

RTA-13 EWTA will provide enterprise wide systems that support the creation, capture, storage, publication and retrieval of documents, images and other information rich objects that are used within agency processes or are exchanged with external organizations and constituents.

### **Standard 3: Novell Directory Services**

Novell Directory Services (NDS e-Directory) is the State's strategic directory service for enterprise-wide directories (i.e. Intranet or Extranet directories, Internet applications, directory-enabled internal applications, network user account management) (*RTA-12, RTA-14*). An assessment will be made of the cost, complexity and benefits of using NDS for direct management via Novell's Account Manager tool of named resources on the installed base of Windows NT and Unix platforms. Over time as the NT platforms are converted to Win2000, their user accounts and resource information will transition to the e-Directory. Platforms that require Microsoft Active Directory (Win2000, Exchange 2000) will be synchronized with NDS using DirXML. An assessment will be made of the cost, complexity and benefits of using the NDS directory to manage the Active Directory for these platforms with Novell's Account

## Collaboration And Directory Services Domain Technical Architecture

Manager tool. The State will aggressively assess the appropriate use of NDS in its overall security framework, including digital certificate management. The State's *Policy for Directory Services* explains the scope of this standard (see Appendix A). Recently initiated projects to pilot the implementation of NDS in the Win2000 server environment with Exchange 2000 will be used to determine State naming conventions and directory schema (*RTA-11*, *RTA-12*) that will be used in agency and application directories as mandated by the directory services policy. This product supports a number of the conceptual architecture principles including:

- Information is an Enterprise Asset
- Ensure Security
- Confidentiality and Privacy
- Reduce Integration Complexity
- Integration
- Total Cost of Ownership
- Minimize Platform Configurations
- Basic Information Services
- Logical Partitioning and Boundaries
- Mainstream Technologies
- Industry Standards
- Enterprise Network as Virtual LAN
- and Scalability.

RTA-11 EWTA shall provide secure access to all computing and information resources for mobile workers.

RTA-12 EWTA will provide unified directory services that integrate the existing identification, routing, connectivity, and access control functions of our computing environments. Establish common directory services for security, Domain Naming Services, e-mail, authentication, authorization, and device access using enterprise-naming standards.

RTA-14 EWTA will provide comprehensive security and confidentiality mechanisms as well as access rights management to ensure compliance with contractual, regulatory and other legal information requirements.

### **Standard 4: Simple Mail Transport Protocol (SMTP)**

Simple Mail Transport Protocol (SMTP) is the State's standard transport protocol for sending messages from one MTA to another MTA over the Internet (*RTA-10*). Using MIME encoding, it enables the transfer of text, video, multimedia, images, and audio attachments. It is the predominant transfer protocol utilized by e-mail user agents.

RTA-10 EWTA will provide support for productive teamwork including file sharing, email, application sharing, white boarding, audio and video conferencing, and work routing.

### **Standard 5: Multi-purpose Internet Mail Extensions (MIME)**

Multi-purpose Internet Mail Extensions (MIME), a SMTP message structure, is the State's standard specification for the attachment of audio, video, image, application programs, and ASCII text messages (*RTA-3*, *RTA-10*). It defines a structured format for messages which allows a single message to contain many parts. The content type is stored in the message header as mail extensions. When the message is delivered the player or application specific to the content type is opened so that the attachment can be viewed in its native format. If the player or application is not included with the browser, then the user must load it. Common image and video players are



## Collaboration And Directory Services Domain Technical Architecture

included with most browsers. S/MIME (Secure MIME) is supported for situations where digitally signed and encrypted Internet mail is required. S/MIME was originally developed by RSA Data Security, Inc. It is based on the PKCS #7 data format for the messages, and the X.509v3 format for certificates. PKCS #7, in turn, is based on the ASN.1 DER format for data.

RTA-3 EWTA will enable direct constituent access, from multiple locations, via multiple methods and media, to appropriate information.

RTA-10 EWTA will provide support for productive teamwork including file sharing, email, application sharing, white boarding, audio and video teleconferencing, and work routing.

### **Standard 6: Lightweight Directory Access Protocol (LDAP)**

Lightweight Directory Access Protocol (LDAP) is the State's standard directory access protocol (*RTA-12*). LDAP is based on Directory Access Protocol (DAP), an X.500 standard access protocol. X.500 is a set of CCITT/ITU standards for electronic directory services. LDAP has been proven to be more efficient for transactions between Mail User Agents and directory services. In addition, LDAP can be utilized to access databases other than the email directories, which will add value to other Collaboration Technologies applications, such as scheduling.

RTA-12 EWTA will provide unified directory services that integrate the existing identification, routing, connectivity, and access control functions of our computing environments. Establish common directory services for security, Domain Naming Services, e-mail, authentication, authorization, and device access using enterprise-naming standards.

### **Standard 7: Extensible Markup Language (XML)**

Extensible Markup Language (XML) is the State's standard for cross platform data encoding and formatting. It is the data exchange standard embedded in Novell's DirXML product, which is specifically designed to allow the integration of directory services. DirXML ships with drivers that can be used to connect NDS eDirectory to Lotus Notes, Microsoft Active Directory, Microsoft Exchange, and older versions of Novell Directory Services (NDS). NDS eDirectory and DirXML are the products specified in the State's policy for Directory Services (see Appendix A).

Extensible Markup Language describes a class of data objects called XML documents and partially describes the behavior of computer programs which process them. XML is an application profile or restricted form of SGML, the Standard Generalized Markup Language that was specifically defined for use in the Web environment. XML has been widely accepted by the IT industry as a viable integration method.

"XML is primarily intended to meet the requirements of large-scale Web content providers for industry-specific markup, vendor-neutral data exchange, media-independent publishing, one-on-one marketing, workflow management in collaborative authoring environments, and the processing of Web documents by intelligent clients. It is also expected to find use in certain metadata applications. The language is designed for the quickest possible client-side processing consistent with its primary purpose as an electronic publishing and data interchange format."

[971208 W3C press release]

See also the discussion of XML in the Middleware Architecture for a broader understanding of the role of XML and related standards in the delivery of integration services.

### **Standard 8: Novell DirXML**

DirXML is Novell's data sharing and synchronization product for automatically distributing new and updated information within a matrix of linked directories, applications and databases. This product will allow the State to designate authoritative sources for data, for example the Human Resource System (HRS) that will maintain personnel data, that can be replicated via the Statewide e-Directory to all appropriate directories and systems. This method could be used to create user accounts and establish access rights to network resources and applications based on roles, work locations and rules defined within the HRS system. Benefits of this approach include elimination of redundant data entry and rapid provisioning of IT-based resources required by State employees to perform their job functions.

### Ongoing architecture Development

The following component technologies or applications of technologies were not addressed for this version of the domain architecture, but will be in the work plan for the next routine update.

#### **Imaging**

There are several current projects, including a major initiative at the Department of Revenue Services that will benefit from the development of design principles and best practices for the appropriate use of various detailed technical standards for imaging technologies. Imaging was an evaluation element of the Integrated Document Management RFP. A decision needs to be made as to whether FileNET's proposed products will be the only strategic products for the State (Panagon IDM Image Services and Panagon Document Services Capture Desktop are available via the Statewide contract). There is an unresolved issue regarding the cost of establishing and staffing a centralized support program for small systems.

#### **Computer Output to Laser Disk**

COLD was an evaluation element of the Integrated Document Management (IDM) RFP. A decision needs to be made as to whether FileNET's proposed product (Panagon IDM Report Manager Services) will become the state standard or simply the preferred solution in situations where Panagon IDM is or will be deployed.

#### **Content Management**

This is an applied technology area, much like knowledge management, that is shared with the E-Government domain. Ongoing collaborative work between these two domains will begin to shape best practices and technical standards for this area.

In general, across all domains, there is a need to define a rigorous, well documented technology assessment process and a staffing plan that will facilitate deeper exploration of detailed architecture specifications such as standardized configurations and ongoing research and analysis by the domain teams. This is especially important for this domain because the component technologies are in constant churn as the developers add new functionality and compete for market share. In the realm of collaborative technologies there may be some built-in functions we chose to forgo because they conflict with the architecture principles, introduce complexity, increase support costs without business value, create risk for the fulfillment of our information stewardship responsibilities, or are better served with other component technologies.

#### **Workflow Integration**

Workflow standards developed by the Workflow Management Coalition are expected to provide interoperability between workflow software and applications as well as between different workflow systems. As is normally the case, international standards are not consistently implemented from one product to the next. Careful assessment of integration issues will be necessary especially to facilitate decisions for multi-agency event-driven systems such as CORE-CT and the CJIS-Offender Based Tracking System.

#### **Electronic Mail Response Management**

The mail response management market is evolving rapidly and will be subsumed within the broader market that is focused on managing interactions with customers. The Web E-Government domain and the Collaboration domain will work together on this area. The State's approach to managing its interactions with citizens must include self-service tools for the Web

## Collaboration And Directory Services Domain Technical Architecture

environment and collaborative tools for the human agents that respond to requests for assistance, regardless of whether the contact is via the Web, telephone or face-to-face.

### **Directory Services**

Much work remains to be done across all the domains to explore evolving international standards and conduct formal technology assessments.

## Emerging Standards

The following international standards are being tracked because they support the realization of the following Conceptual Architecture Principles.

### ***Integration***

Systems must be designed, acquired, developed, or enhanced such that data and processes can be shared and integrated across enterprises and with our partners.

### ***Industry Standards***

Priority will be given to products adhering to industry standards and open architecture.

As these standards are implemented in mainstream groupware products we can explore interoperability testing between the State's Exchange 2000 / Outlook 2000 environment and external organizations for whom cross-organizations scheduling would improve our coordination of work. External organization could include our program service partners and regulated entities.

## **Emerging 1: Internet Calendaring and Scheduling Core Object Specification (iCalendar)**

The Internet Calendaring and Scheduling Core Object Specification, or iCalendar, allows for the capture and exchange of information normally stored within a calendaring and scheduling application; such as a Personal Information Manager (PIM) or a Group Scheduling product. RFC 2445 provides the definition of a common MIME format for openly exchanging calendaring and scheduling information across the Internet. The RFC defines the format for specifying iCalendar object methods. An iCalendar object method is a set of usage constraints for the iCalendar object. For example, these methods might define scheduling messages that request an event be scheduled, reply to an event request, send a cancellation notice for an event, modify or replace the definition of an event, provide a counter proposal for an original event request, delegate an event request to another individual, request free or busy time, reply to a free or busy time request, or provide similar scheduling messages for a to-do or journal entry calendar component. The content type is suitable as a MIME message entity that can be transferred over MIME based email systems, using HTTP or some other Internet transport.

## **Emerging 2: iCalendar Transport-Independent Interoperability Protocol (iTIP)**

Scheduling Events, BusyTime, To-dos and Journal Entries. RFC 2446 specifies how calendaring systems use iCalendar objects to inter-operate with other calendar systems. It does so in a general way so as to allow multiple methods of communication between systems. Subsequent documents specify interoperable methods of communications between systems that use this protocol. The document outlines a model for calendar exchange that defines both static and dynamic event, to-do, journal and free/busy objects. Static objects are used to transmit information from one entity to another without the expectation of continuity or referential integrity with the original item. Dynamic objects are a superset of static objects and will gracefully degrade to their static counterparts for clients that only support static objects. This document specifies an Internet protocol based on the iCalendar object specification that provides scheduling interoperability between different calendar systems. The Internet protocol is called the "iCalendar Transport-Independent Interoperability Protocol (iTIP)".

## Collaboration And Directory Services Domain Technical Architecture

iTIP complements the iCalendar object specification by adding semantics for group scheduling methods commonly available in current calendar systems. These scheduling methods permit two or more calendar systems to perform transactions such as publish, schedule, reschedule, respond to scheduling requests, negotiation of changes or cancel iCalendar-based calendar components. iTIP is defined independent of the particular transport used to transmit the scheduling information. Companion memos to iTIP provide bindings of the interoperability protocol to a number of Internet protocols.

### **Emerging 3: iCalendar Message-Based Interoperability Protocol (iMIP)**

RFC 2447 specifies a binding from the iCalendar Transport-independent Interoperability Protocol (iTIP) to Internet email-based transports. This binding document provides the transport specific information necessary convey iCalendar Transport-independent Interoperability Protocol (iTIP) over MIME as defined in RFC-822 and RFC-2045.

### Collaboration & Directory Services Product Status

The following table categorizes products currently found in the State's installed base of technologies or under consideration for use by the State. The four categories used, Obsolete, Transitional, Strategic and Research are defined as follows:

#### OBSOLETE

It is highly likely that these standards or products, while still in use, will not be supported by the vendor (industry, manufacturer, etc.) in the future. Some products and standards have already reached the non-supported state. Plans should be developed by the agencies or the State to rapidly phase out and replace them with strategic standards or products. No development should be undertaken using these standards or products by either the agencies or the State.

#### TRANSITIONAL

These are standards or products in which an agency or the State has a substantial investment or deployment. These standards and products are currently supported by DOIT, the agencies, or the vendor (industry, manufacturer, etc.). However, agencies should undertake development using these standards or products only if there are no suitable alternatives that are categorized as strategic. Plans should be developed by the agencies or the State to move from transitional to strategic standards or products as soon as practical. In addition, the State should not use these standards or products for development.

Note: many older versions of *strategic* standards or products fall into this category, even if not specifically listed in a domain architecture document.

#### STRATEGIC

These are the standards and products selected by the state for development or acquisition, and for replacement of obsolete or transitional standards or products. (Strategic means a three to four year planning horizon.) When more than one similar strategic standard or product is specified for a technology category, there may be a preference for use in statewide or multi-agency development. These preferred standards and products are indicated where appropriate.

Note: some strategic products may be in "pilot testing" evaluation to determine implementation issues and guidelines. Pilot testing must be successfully completed prior to full deployment by the agencies or the State.

#### RESEARCH / EMERGING

This category represents proposed strategic standards and products that are in advanced stages of development and that should be evaluated by the State. Some of these standards or products may already be undergoing "hands-on" evaluation. Others will need to be tracked and evaluated over the next 6 to 18 months.

## Collaboration And Directory Services Domain Technical Architecture

<b>Product</b> Existing or Proposed	<b>Obsolete</b>	<b>Transitional</b>	<b>Strategic</b>	<b>Research</b>
<b>Basic Collaboration:</b> E-Mail; Calendar Sharing/Scheduling; Network-based Fax				
Banyan Intelligent Messaging & Beyond Mail	✓			
CC:Mail	✓			
Exchange 2000			Pilot	
Exchange – old versions		✓		
Groupwise – all versions		✓		
Lotus Notes - Mail & Calendar		✓		
MS Mail		✓		
Outlook 2000			Pilot	
Outlook – old versions		✓		
Outlook Express		✓		
State e-mail Web Interface		✓		
TAO		✓		
<b>Extended Collaboration</b>				
CaLANdar	✓			
Exchange 2000			Pilot	
Exchange – older versions		✓		
GroupWise – all versions		✓		
Lotus Notes - Workgroup		✓		
FileNET Panagon Integrated Document Management (IDM) - for document management			✓	
FileNET Panagon IDM and Capture Desktop – for low volume imaging (under 10,000 pages/day)			✓	
FileNET Panagon IDM Image Services – for high volume imaging			✓	



## Collaboration And Directory Services Domain Technical Architecture

<b>Product</b> Existing or Proposed	<b>Obsolete</b>	<b>Transitional</b>	<b>Strategic</b>	<b>Research</b>
<b>Process Management</b>				
Exchange 2000				✓
FileNET Workflow			✓	
GroupWise – all versions		✓		
Lotus Notes – Workflow applications		✓		
<b>Directory Services</b>				
Active Directory – Mail Account Mgmt for Exchange 2000			Pilot	
Active Directory – Server Sharing Mgmt for Win2000			Pilot	
Banyan StreetTalk	✓			
NDS eDirectory			Pilot	
Novell DirXML			Pilot	
NDS – older versions		✓		
NT Server Native Directory		✓		
Unix Server Native Directory				✓

## Appendix A: Implementation and Deployment of Directory Services

### Implementation and Deployment of Directory Services

**Version: 1.00**

**DATE ISSUED:** December 8, 2000

**Date Revised:**

**DATE EFFECTIVE: Dec. 11, 2000**

**Supersedes:**

[Policy Statements](#) | [Implementation](#) | [Planning and Reporting](#) | [Scope](#) | [Definitions](#)

#### Purpose

The CIO for the State of Connecticut is establishing this policy, planning and reporting requirements and associated standards. The policy statements are designed to provide consistency in the deployment of directories and directory enabled applications, and to ensure that the appropriate resources can be provided in a timely and efficient manner. This will reduce the overall total costs of ownership and will facilitate the support and management of directory services.

#### Policy Statements

Enterprise-wide Intranet or extranet directories, and Internet application directories will use the State standard directory services. These services utilize Novell NDS Corporate Edition and eDirectory.

Application servers based on Windows NT or Unix will utilize the State standard directory services in preference to local or system level directory and authentication services. Application servers based on Windows 2000 will use Active Directory; synchronized and managed using Novell NDS Corporate Edition or eDirectory.

The management and synchronization of directories will use the facilities of Novell NDS Corporate Edition and eDirectory products. The protocols used will be the current State standards. At present, these are LDAP and DirXML.

Agencies deploying directory-enabled applications or business systems will work with DOIT on the best choice of directory services to be utilized. Preference will be given to solutions either directly use Novell NDS Corporate Edition or eDirectory, or are capable of being synchronized with directories created using those products.

Naming conventions and directory schema used in agency and application directories will follow the State naming conventions and directory schema.

#### Agency Planning and Reporting Responsibilities

##### Planning:

1. Agency IT planning should be adjusted to reflect an anticipated rollout date of early 1Q2001 for Novell NDS Corporate Edition or eDirectory services.
2. Agencies wishing to participate in an evaluation of Novell NDS Corporate Edition or eDirectory services should contact their DOIT representative.

## Collaboration And Directory Services Domain Technical Architecture

3. DOIT and the agencies will need to work out a plan for establishing who is the authoritative source for changes to directory contents

### **Reporting:**

TBD

### **Implementation:**

This policy applies to all:

- New or replacement Local Area Networks
- New or replacement E-mail (other than POP3) and groupware implementations.
- New directory enabled applications intended for Intranet or Internet use (as determined by DOIT and the implementing agency or agencies).

**Certification:** N/A

### **Scope**

This policy applies to the following entities: any State of Connecticut agency, institution, office, department, commission, council or instrumentality subject to the policies, standards and decisions of the Chief Information Officer of the Department of Information Technology as specified in Public Act 97-9).

### **Definitions**

#### **State Agency:**

For the purposes of this policy, the term State Agency refers to any State of Connecticut agency, institution, office, department, commission, council or instrumentality.

#### **Compliant:**

For the purposes of this policy, an Internet or web site or extranet site is considered compliant when it meets the criteria defined in this policy and the network security policy.